

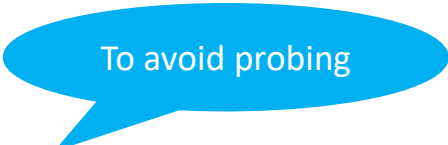
# DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)

<https://tools.ietf.org/html/draft-ietf-add-dnr>

March 2021

M. Boucadair (Orange)  
T. Reddy (McAfee)  
D. Wing (Citrix)  
N. Cook (Open-Xchange)  
Tommy Jensen (Microsoft)

# Proposal

- If DNSSEC is supported by the client
  - The client uses {ADN+IP Address List}
  - Then, issues SVCB queries to that list to resolve discovered ADN(s)
- If DNSSEC is not supported
  - The client uses {ADN+IP Address List+Port+Encrypted DNS Flags} returned in DNR option(s)
  - If the client supports both DoT and DoH (or both DoQ and DoH), the client established a DoT (or DoQ) connection and uses SVCB to retrieve the URI Templates *assuming the resolver supports DoT or DoQ*
  - If DoH-only, the client MUST add “URI Templates” to the list of requested information
    - To avoid external attacks, including SVCB blocking

# Proposal: Simplified

- **DoH implementations MUST support DoT**
- If DNSSEC is supported by the client
  - The client uses {ADN+IP Address List}
  - Then, issues SVCB queries to that list to resolve discovered ADN
- If DNSSEC is not supported
  - The client uses {ADN+IP Address List+Port+Encrypted DNS Flags} returned in DNR option(s)
- ~~— If the client supports both DoT and DoH (or both DoQ and DoH), the client established a DoT (or DoQ) connection and uses SVCB to retrieve the URI Templates *assuming the resolver supports DoT or DoQ*~~
- ~~— If DoH only, the client MUST add “URI Templates” to the list of requested information~~
  - ~~• To avoid external attacks, including SVCB blocking~~

# Proposal: Simplified (Not an Option)

- DoH implementations **MUST** support DoT

This updates RFC8484

This is beyond the WG charter that is about discovery not about imposing capabilities of discovered servers

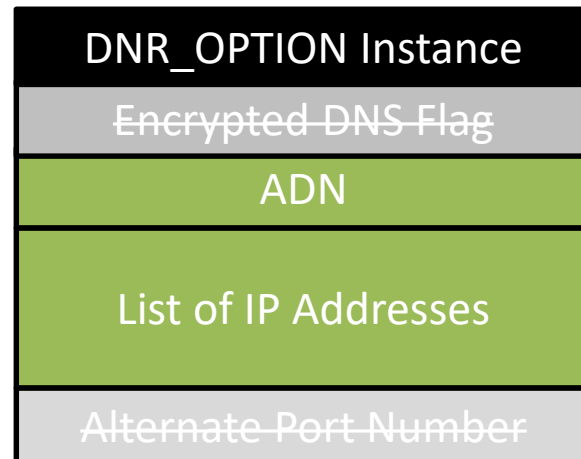
# How To Achieve the Intended Behavior with the Same Option(s)?

The client supports DNSSEC

Request

DNR\_OPTION

Response



MUST be  
ignored  
by the  
client

# How To Achieve the Intended Behavior with the Same Option(s)?

The client does not support DNSSEC but at least DoT or DoQ are supported:

Request

DNR\_OPTION

Response

DNR\_OPTION Instance

Encrypted DNS Flag

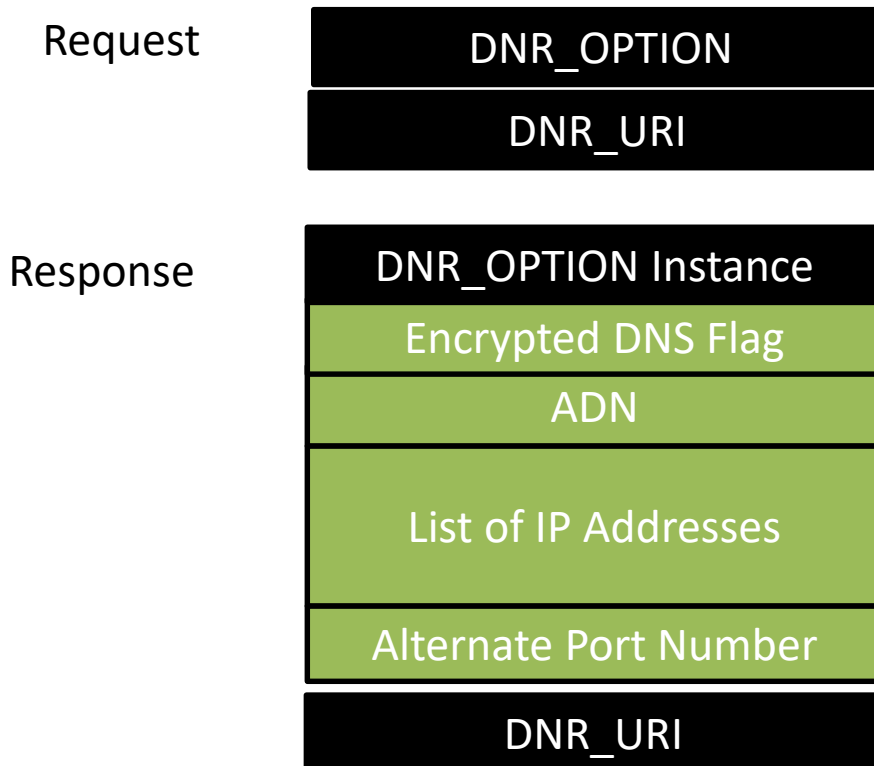
ADN

List of IP Addresses

Alternate Port Number

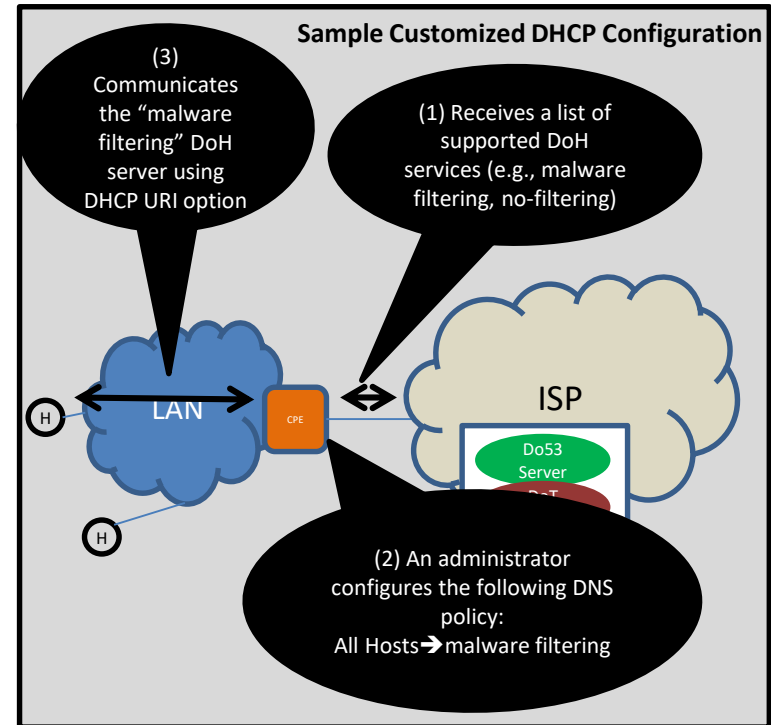
# How To Achieve the Intended Behavior with the Same Option(s)?

The client does not support DNSSEC + DoH-only (client):



# Issue: Customized Local URI Templates

- Why?
  - Provide a customized DNS configuration within a local network
- Advantage
  - Does *not interfere* with DNS exchanges to “customize” the available services
  - If the CPE is not acting as a forwarder for the encrypted DNS, it has no means to enforce the policy



## Suggestions:

- Define RA/DHCP options to convey URI Templates
- These options, when available, take precedence over DDR



# Next Steps

- Implement the outcome of the discussion
- Edits and clarification to take into account Michael and Yan's comments
  - <https://github.com/ietf-wg-add/draft-ietf-add-dnr/issues/>
- Please review and share comments

# Backup

# Sync DDR and DNR

- DHCP servers can issue SVCB queries and cache the results
  - That cache can be used to populate the DHCP options
  - See, for example, [RFC 7969](#)
- " Depending on the server capability and configuration, it may cache resolved responses for a specific period of time, repeat queries every time, or even keep the response until reconfiguration or shutdown. For more detailed discussion, see Section 7 of [RFC7227]."